# High-performance Implementation Approach of Elliptic Curve Cryptosystem for Wireless Network Application

Abdalhossein Rezai[1], Parviz keshavarzi[2]

Electrical and Computer Engineering Faculty, Semnan University,Semnan, Iran

[1]a_h_rezai@sun.semnan.ac.ir; [2]pkeshavarzi@semnan.ac.ir

***Abstract*-This paper presents a new efficient implementation approach of elliptic curve cryptosystem based on a novel finite field multiplication and a high performance scalar multiplication algorithm for wireless network authentication. In this new finite field multiplication, CLNZ sliding window method is used on the signed-digit multiplier in order to reduce the multiplication steps. In addition, in scalar multiplication algorithm of the proposed implementation approach, point addition and point doubling operation compute in parallel. In addition, window technique and signed-digit representation are used in order to reduce the number of point operation. So the multiplication cost in the proposed implementation approach reduced considerably. Using this new implementation approach, the security of the elliptic curve cryptosystem increased considerably. The results show that the proposed finite field multiplication reduces the number of multiplication steps at about 40%-82.4% for d=2-10 in compare with Montgomery modular multiplication algorithm. In addition, the efficiency of the proposed implementation approach of elliptic curve cryptosystem enhances about 88%-97% in compare with the implementation approach of traditional window NAF elliptic curve scalar multiplication algorithm and enhances about 77% in compare with the implementation approach of window NAF elliptic curve scalar multiplication algorithm (based on interleaving) where w=4 and 8, and d=8.**

***Keywords-Wireless Network Security; Authentication; Elliptic Curve Cryptosystem; Scalar Multiplication; Finite Field Multiplication; Signed-digit Recoding***

## I. INTRODUCTION

In the recent years, wireless networks and mobile devices such as cell phone, PDA and smart card, are widely used. So the security of wireless networks and mobile devices becomes an increasing concern [1]-[3]. In wireless networks, remote user authentication in insecure channel is an important issue [1]. Due to the limitation in the bandwidth, computational strength, power availability or storage in mobile devices, the PKC-based remote authentication schemes are not suitable for mobile devices [1]-[2]. So, several authentication schemes based on elliptic curve cryptography (ECC) are proposed [4], [5]-[6]. For example, wireless transport layer security (WTLS) of wireless application protocol (WAP) using elliptic curve Diffi-Hellman (ECDH) authentication algorithm in order to authenticate client and server.

ECC was developed in 1985 independently by Koblitz [7] and Miller [8]. The security of the ECC is based on the intractability of the elliptic curve discrete logarithm problem (ECDLP) [9]. Compared with RSA, ECC offers a better performance due to a smaller key size with the same security [1], [9]-[10].

In ECC-based authentication algorithm, elliptic curve scalar multiplication is core operation, but this operation is the most time consuming operation. This operation takes 85% of executing time [11].

Hardware implementation of ECC involves tree-layer hierarchical strategy namely finite field arithmetic, point arithmetic and scalar multiplication as shown in Fig. 1 [9].

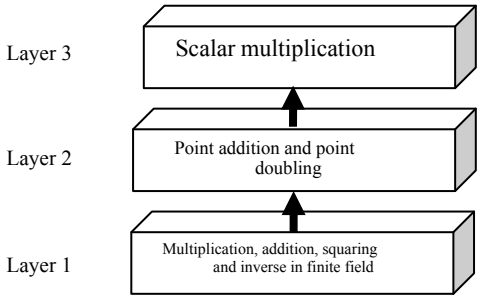


Fig. 1. Three-layer Model for Elliptic Curve Scalar Multiplication [9]

There are many attempts to implement these three layers in order to obtain fast computation, reduce power consumption and reduce storage space such as double-base chain [12], parallel structure [9]-[10], [13]-[14], recoding technique[15]-[16] and high-radix multiplier [17]-[18].

In this paper, a novel finite field multiplication algorithm based on constant length nonzero (CLNZ) sliding window method, multiple bit scan, multiple bit shift and signed-digit technique is presented. This new finite field multiplication algorithm is an improvement of the multiplication method in [19]. In addition we proposed using this new finite field multiplication in order to speeding up the elliptic curve scalar multiplication algorithm. So the efficiency and the security of the wireless network authentication increased considerably.

The rest of this paper is organized as follows: section II describes the methods of scalar multiplication and the adaptive m-ary canonical recoding multiplication method. The proposed finite field multiplication algorithm and its application in window elliptic curve scalar multiplication algorithm are presented in section III. Section IV evaluates the proposed algorithms. Finally conclusion is given in section V.

## II. BACKGROUND

### A. The Methods of Scalar Multiplication

The scalar multiplication is achieved by repeated point addition (PA) and point doubling (PD) operations. The binary method which is shown in Fig. 2, is well known method to perform the scalar multiplication of $Q = kP$ [20].

**INPUT:** $k \in [1, n-1]; P \in GF(2^n)$;
**OUTPUT:** $Q = kP$;
1. $Q \leftarrow 0$;
2. **For** $i = 0$ **to** $n-1$
3. **If** $k_i = 1$ **then** $Q \leftarrow Q + P$;
4. $P \leftarrow 2P$;
5. **Return** $Q$;

Fig. 2. The Binary Scalar Multiplication Method [20]

In this method, for $n$-bit random $k$, the expected number of PA and PD is $\frac{n}{2}$ and $n$ respectively. The cost of multiplication in binary multiplication method depends on the Hamming weight and length of the binary representation of k. So binary method can be improved by scanning few bits at a time as with sliding window method [11] and non adjacent form (NAF) of integers [14], [16], [20]. One of the efficient methods for reduce the cost of computation is window scalar multiplication method [16] which is shown in Fig. 3

In this algorithm, sliding window method and signed-digit representation is used in order to reduce the cost of multiplication. In evaluation stage of this algorithm, when $u_i \neq 0$, the point $Q_u$ is computed in which $u$ satisfying $a_u = u_i$ or $a_{-u} = -u_i$. Scalar multiplication will cost $\frac{m}{w+1}A$ in step 4, and in step 5 will cost $\sum_{j=1}^{v} \frac{l_j}{w_j + 1} A$, where $A$ denotes PA cost, $D$ denotes PD cost, $w$ denotes window width and $l_j$ denotes the length of $NAF_{wj}$.

### *B. The Adaptive M-ary Canonical Recoding Multiplication Method*

The m-ary method and canonical recoding are two well-known methods in order to reduce the total number of the additions in multiplication of two integers. The m-ary (radix-m) method utilizes segmentation and pre-computation in order to reduce the number of addition [14], [19], [21]-[22]. Since in binary representation, the probability of a word with d-bit zero in sequence is $2^{-d}$, longer words have smaller probabilities. For increase efficiency of the probability, Koc and Hung in [19] proposed an adaptive m-ary method which allows zero words are variable lengths and improve zero word probability while using relatively long words in the segmentation process.

According to [19], in computing $P = X.Y$, we may skip additions whenever the corresponding bit of the multiplier is zero. So, the binary multiplication algorithm and canonical recoding multiplication algorithm require on average $\frac{n}{2}$ and $\frac{n}{3}$ addition operation respectively. Koc and Hung in [19] proposed the combination of the adaptive m-ary segmentation algorithm and the canonical recoding algorithm in order to obtain the adaptive m-ary segmentation canonical recoding multiplication algorithm which is shown in Fig. 4.

**INPUT:** $w; k \in [1, n-1]; P \in GF(2^n)$;
**OUTPUT:** $Q = kP$;
1. Use algorithm 3 (in appendix [16]) to compute $\rho' = k \ part \bmod \delta$;
2. Use algorithm 4 (in appendix [16]) to compute $\tau NAF_w(\rho') = \sum_{i=0}^{l-1} u_i \tau^i$;
3. **For** $u \in U = \{1,3,5,...,2^{w-1}-1\}$ **let** $Q_u \leftarrow \infty$;
4. **For** $i = l-1$ **to** 0
   4.1. **If** $u_i \neq 0$ **then**
      **Let** $u$ satisfying $a_u = u_i$ or $a_{-u} = -u_i$;
      **If** $u > 0$ **then** $Q_u \leftarrow Q_u + P$;
      **Else** $Q_{-u} \leftarrow Q_{-u} - P$;
   4.2. P $\leftarrow \tau$P;
5. **Compute** $Q \leftarrow Q + \sum_{u \in U} u_i Q_u$;
6. **Return** $Q$;

Fig. 3. The Window Scalar Multiplication Method [16]

**Input:** $X, Y$;
**Output:** $P = X.Y$;
*{Recoding phase}*
1. **Compute** $D$ by performed canonical recoding on $X$;
*{Pre-computation phase}*
2. **Decompose** $D$ into $X$ * by using adaptive m-ary method;
3. **Compute** and **store** $w.Y$ for all canonically recoded d-digit numbers of $D$;
*{Multiplication phase}*
4. **Set** $j = 0$ and $X_0^* = \emptyset$;
5. **For** $i = 0$ **to** $n-1$ do one of the following:
6. Case 0. ($X_j^* = \emptyset$) append $X_i$ to $X_j^*$;
7. Case 1. ($X_j^* \in W_0$ *and* $X_i$ *is zero*) append $X_i$ to $X_j^*$;
8. Case 2. ($X_j^* \in W_0$ *and* $X_i$ *is nonzero*) set $j = j+1$ and $X_j^* = X_i$;
9. Case 3. ($X_j^* \in W_1$ *and* $1 \le l_j \le d-2$) append $X_i$ to $X_j^*$;
10. Case 4. ($X_j^* \in W_1$ *and* $l_j = d-1$) append $X_i$ to $X_j^*$; Set $j = j+1$ and $X_j^* = \emptyset$;
11. **Set** $k = j+1$ and $P = 0$;
12. **For** $j = k-1$ **to** 0
13. **Compute** $P = 2^{l_j} P + X_j^* Y$;
14. **Return** ($P$);

Fig. 4. The Adaptive M-ary Segmentation Canonical Recoding Multiplication Algorithm [19]

In this algorithm, $l_j$ denotes the length of $X_j^*$. The probability of the zero bits is also increased by using canonical recoding technique and the total computation time is reduced by using m-ary segmentation.

## III. THE PROPOSED IMPLEMENTATION APPROACH OF ELLIPTIC CURVE CRYPTOSYSTEM

In this section, we proposed a new efficient implementation approach of elliptic curve cryptosystem based on parallel structure and new efficient finite field multiplication for layer 3 and 1 of the Fig. 1 respectively.

### A. Scalar Multiplication

The basic operations in all scalar multiplication algorithms are point addition and point doubling over an elliptic curve. By parallel execution of these point operations, the speed and the security of the cryptosystem increased considerably. So we use window scalar multiplication algorithm in [16] in order to parallel execution of these point operations. But we proposed an efficient finite field multiplication algorithm in order to speed up this scalar multiplication algorithm.

### B. The Finite Field Arithmetic

Modular multiplication is major finite field arithmetic. So the performance of ECC depends heavily on the efficiency of the modular multiplication in finite field [9]-[10].

In finite field multiplication, partial result shifts one bit per iteration. Also multiplication by zero bit results in zero, but this multiplication by zero is performed and implemented in the each iteration. In this paper, we proposed a new modified Montgomery modular multiplication by recoding the multiplier and then partitioning this signed-digit multiplier and performed multiplication by zero partition with any length in only one-cycle instead of several cycles. The proposed modified Montgomery modular multiplication (M4) algorithm is shown in Fig. 5:

In this algorithm $l_j$ is the length (i.e. number of bits) of ith partition, $\#\Pi(D)$ is the number of partitioning in the multiplier and $V_i$ is the corresponding partition value.

In recoding phase of this new algorithm, the canonical recoding is performed on the multiplier. In partitioning phase, the CLNZ partitioning is performed on the signed-digit multiplier, so the number of zero partitions is as large as possible, thus the number of multiplication steps is reduced considerably. In this algorithm, the CLNZ partitioning method scans the multiplier from the least significant digit to the most significant digit according to the algorithm which is shown in Fig. 6. Using this strategy, zero windows are allowed to have an arbitrary length, but the maximum length of nonzero windows should be the exact value of d digit.

For example, for $X = (0111111100111111101)_2$, the canonical recoding of $X$ is $D = (0100000\bar{1}0100000\bar{1}01)$ and for $d = 3$, the window formed will be $\Pi(D) = (001), (000000), (\bar{1}01), (000000), (\bar{1}01)$.

In pre-computation phase of the proposed M4 algorithm, the least significant digit of nonzero partition is either 1 or $\bar{1}$, which implies that the nonzero partition value is always an odd number. So we only require pre-computation of $V_iY$ for odd number of $V_i$.

In this new M4 algorithm, pre-computation phase and partition phase is performed independently in parallel which is speeding up modular multiplication.

The multiplication phase of M4 algorithm is performed $w$ times. Recall that; $w$ denote the number of partitioning in the signed-digit multiplier. In each iteration of the multiplication phase of M4 algorithm, $l_i$ bits of multiplier and n-bit multiplicand are processed.

**Input:** $X, Y, M$;

**Output:** $P := X.Y.2^{-n} \bmod M$;

1. $P = 0$;

*{Recoding phase}*

2. **Compute** $D$ by performed canonical recoding on $X$ ;

***Parallel begin***

*{Partitioning phase}*

3. **Building** $\Pi(D)$ using the given strategy;
4. **Let** $w = \#\Pi(D)$;

*{Pre-computation phase}*

5. **Compute** and **store** $V_iY$;

***Parallel end***

*{Multiplication phase}*

6. **For** $i = 0$ **to** $w - 1$
7. $P := P + V_iY$ ;
8. $m := P_0 M'_0 \bmod 2^{l_i}$ ;
9. $P := (P + m.M) / 2^{l_i}$ ;
10. **If** ( $P > M$ ) **then** $P := P - M$ ;
11. **Return** ( $P$ );

Fig. 5. The New Modified Montgomery Modular Multiplication (M4) Algorithm

**Input:** $D, d$;

**Output:** $\Pi(D)$ ;

**ZP:** check the incoming single digit;
If it is zero then stay in ZP
Else go to NZP;
**NZP:** stay in NZP until all d digits are collected;
Check the incoming single digit;
If it is zero then go to ZP
Else go to NZP;
**Return** ( $\Pi(D)$ )

Fig. 6. Partitioning Strategy

## IV. EVALUATION

### A. Evaluation of M4 Algorithm

In the proposed modified Montgomery modular multiplication (M4) algorithm, we use signed-digit recoding technique and CLNZ sliding window method. So the Hamming weight of multiplier is $\frac{3n}{3d+4}$. Thus at least, M4 algorithm reduces the multiplication steps at about:

$$1 - \frac{\frac{6n}{3d+4}}{n} = 1 - \frac{6}{3d+4} \quad (1)$$

Table I shows the multiplication step reduction of M4 algorithm in compare with Montgomery modular multiplication algorithm [23] for various d.

TABLE I
MULTIPLICATION STEP IMPROVEMENT OF M4 ALGORITHM OVER MONTGOMERY MODULAR MULTIPLICATION

| d= | Multiplication step reduction (%) | d= | Multiplication step reduction (%) |
|---|---|---|---|
| 2 | 40% | 7 | 76% |
| 3 | 53.8% | 8 | 78.6% |
| 4 | 62.5% | 9 | 80.6% |

| | | | |
|---|---|---|---|
| 5 | 68.4% | 10 | 82.4% |
| 6 | 72.7% | | |

As it is shown in table I the M4 algorithm reduces the multiplication steps at about 40%-82.4% for d=2-10.

### B. *Evaluation of the Proposed Implementation Approach*

According to the computational analysis of [16], the implementation approach of the traditional window NAF (TWN) scalar multiplication algorithm will cost:

$$D+(2^{w-2}-1)A+\frac{m}{w+1}A+mD \qquad (2)$$

In addition, the implementation approach of the window scalar multiplication algorithm based on interleaving (IWN) will cost:

$$\frac{m}{w+1}A+\sum_{j=1}^{v}\frac{l_j}{w_j+1}A \qquad (3)$$

The cost of point addition (PA) and point double (PD) operation equals at affine coordinate. But the cost of PA operation is twice as much as the one of PD operation at projective coordinate [16]. The proposed implementation approach of elliptic curve cryptosystem using combination of M4 algorithm and IWN approach, so proposed implementation approach will cost as IWN approach but the cost of point addition in the proposed implementation approach is reduced considerably.

Assume digit length is m=160 bit. We compare the cost of the proposed implementation approach with the TWN approach and IWN approach by analyzing formula (2) and (3). Fig. 7- 9 show these comparisons for various window width w at affine coordinate and projective coordinate for d=2, 4, 6, 8 and 10.

As it is shown in Fig. 7, Fig. 8 and Fig. 9, the proposed implementation approach is more efficient than TWN approach and IWN approach where window width ( $w$ ) and radix ( $d$ ) are from 2 to 10. When window width $w=4$ and $w=8$ and $d=8$ , we will show comparison of the cost among TWN and IWN approach and the proposed implementation approach by table II and table III where digital length is 160, 192 and 224.

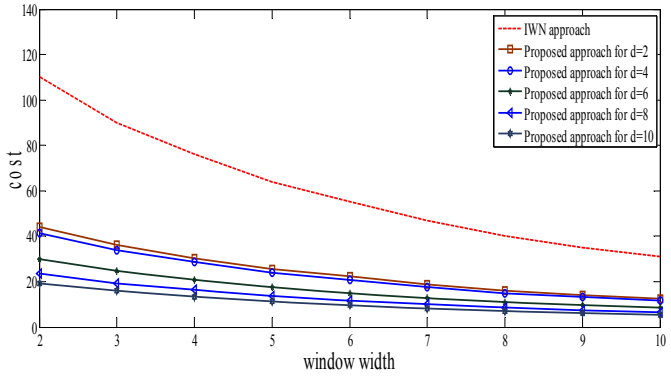


Fig. 7. Comparison of the Cost between the Proposed Implementation Approach and IWN Approach at Affine Coordinate and Projective Coordinates

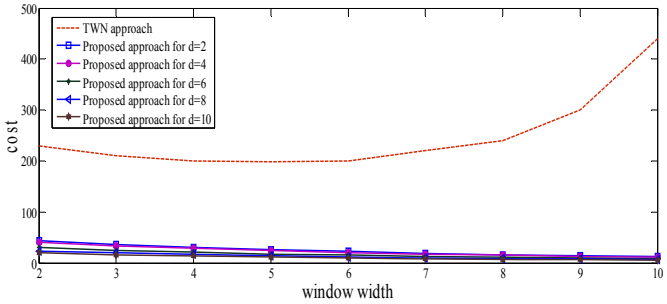


Fig. 8. Comparison of the Cost between the Proposed Implementation Approach and TWN Approach at Affine Coordinate

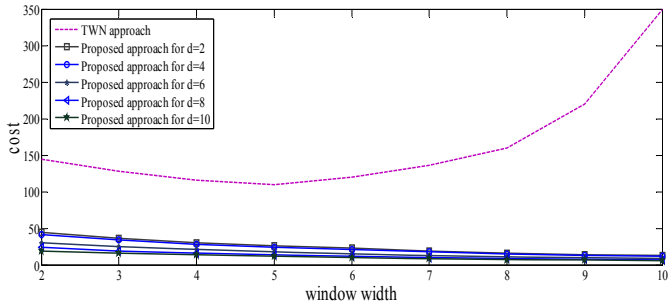


Fig. 9. Comparison of the Cost between Proposed Implementation Approach and TWN Approach at Projective Coordinate

TABLE II
COMPARISON OF THE COST AT AFFINE COORDINATE

| Digit length | Implementation approach | $w$= | |
|---|---|---|---|
| | | 4 | 8 |
| 160 | IWN | 64 | 35.56 |
| | TWN | 196 | 241.78 |
| | Proposed in this paper | 13.7 | 7.61 |
| 192 | IWN | 76.8 | 42.67 |
| | TWN | 234.4 | 277.33 |
| | Proposed in this paper | 16.44 | 9.13 |
| 224 | IWN | 89.6 | 49.78 |
| | TWN | 272.8 | 312.89 |
| | Proposed in this paper | 19.17 | 10.65 |

TABLE III
COMPARISON OF THE COST AT PROJECTIVE COORDINATE

| Digit length | Implementation approach | $w$= | |
|---|---|---|---|
| | | 4 | 8 |
| 160 | IWN | 64 | 35.56 |
| | TWN | 115.5 | 161.28 |
| | Proposed in this paper | 13.7 | 7.61 |
| 192 | IWN | 76.8 | 42.67 |
| | TWN | 137.9 | 180.83 |
| | Proposed in this paper | 16.44 | 9.13 |
| 224 | IWN | 89.6 | 49.78 |
| | TWN | 160.3 | 200.39 |
| | Proposed in this paper | 19.17 | 10.65 |

As it is shown in table II and table III, the efficiency of the proposed implementation approach enhances about 77% in compare with the IWN approach and enhances about 88%-

97% in compare with the TWN approach where $w = 4$ and 8, and $d = 8$.

### C. Security Analysis

In this proposed implementation approach of elliptic curve cryptosystem, PD and PA operation is performed in parallel. In addition, sliding window and recoding technique are used in the scalar multiplication algorithm. So according to [24] the proposed implementation approach of elliptic curve cryptosystem is standing against timing analysis attacks and simple power analysis (SPA) attacks. In addition, in M4 algorithm, recoding technique and CLNZ sliding window method are used. So exploitation of the key information by measurement of the currents flowing thought each component of the cryptography device is hard. Therefore, cryptosystem which use of the proposed implementation approach is standing against electromagnetic analysis (EMA) attacks.

## V. CONCLUSION

In this paper, a novel finite field multiplication algorithm based on signed-digit representation, and CLNZ sliding window method is presented. In this new finite field multiplication, signed-digit is used in order to increase probability of the zero bits and CLNZ sliding window method is used in order to reduce the multiplication steps. In addition, we proposed a new efficient implementation approach of elliptic curve cryptosystem for wireless network authentication based on this new finite field multiplication algorithm. In this new implementation approach, PA and PD operations compute in parallel and both window technique and recoding technique are used in order to reduce the computation cost. Using the proposed implementation approach, the security of the cryptosystem increased considerably.

The results show that the number of multiplication steps in the M4 algorithm is reduced at about 40%-82.4% for d=2-10 in compare with Montgomery modular multiplication algorithm. Also the efficiency of the proposed implementation approach enhances at about 77% and 88%-97% in compare with the IWN approach and TWN approach respectively where w=4 and 8, and d=8.

## REFERENCES


[1] J. Yang and C. Chang, "An ID-based remote mutual authentication with key agreement scheme for mobile devices on elliptic curve cryptosystem," Computers and Security, vol.28, pp. 138-143, 2009.

[2] Y. Xiao-Hui, Q. Fan, Z. Jun, D. Zi-Bin and Z. Yong-Fu, "An optimized scalable and unified hardware stracture of Montgomery Multiplier ," in Proc. The IEEE international conference on E-Business and Information System Security, 2009, pp.1-5.

[3] F. Xiangyan, Z. Jiahang, X. Tinggang and Y.Youguang,"The researcher and implement of high-speed modular multiplication algorithm basing on parallel pipelining," in Proc. the Asia-pacific conference on information processing, 2009, pp.398-403.

[4] P. Abichar, A. Mhamed and B. Elhassan, "A fast and secure elliptic curve based authenticated key agreement protocol for low power mobile communications," in Proc. the international conference on next generation mobile applications, services and technologies, 2007, pp. 235–240.

[5] Y. Liao and S. Wang, "A secure and efficient scheme of remote user authentication based on bilinear pairings," in Proc. the IEEE region 10 conference, 2007, pp. 1- 4.

[6] X. Cao, W. Kou, L. Dang, and B. Zhao, "IMBAS: identity-based multi-user broadcast authentication in wireless sensor networks," Computer Communications, vol.31, pp. 659- 667, 2008.

[7] N. Koblitz, "Elliptic curve cryptosystem," Mathematics of computer, vol .48, pp.203- 209, 1987.

[8] V. Miller, "Uses of elliptic curves in cryptography," in proc. CRYPTO 85, LNCS vol.218, pp. 417- 428, 1985.

[9] N. A. Saqib, F. Rodriguez-Henriquez and A. Diaz-Perez, "A parallel architecture for fast computation of elliptic curve scalar multiplication over GF($2^m$)", in proc. the 18th international parallel and distributed processing symposium, 2004, vol. 4, pp.144a.

[10] S.M. Shohdy, A. B. Elsisi and N. Ismail," Hardware Implementation of efficient modified Karatsuba multiplier used in elliptic curves", International journal of network security, vol.11, no.3, pp.138-145, 2010.

[11] P. G. Shah, X. Huang and D. Sharma, "Sliding window method with flexible window size for scalar multiplication on wireless sensor network nodes," in proc. international conference on wireless communication and sensor computing, 2010, pp. 1- 6.

[12] V. Dimitrov, L. Imbert and P. Mishra, Efficient and secure elliptic curve point multiplication using double-base chains, Lectures Notes in Computer Science, 2005, vol.3788, pp.59- 78.

[13] Y. Dan, X. Zou, Z. Liu , Y. Han and L. Yi, "High-performance hardware architecture of elliptic curve cryptography processor over GF($2^{163}$)," Journal of Zhejiang University - Science A, vol.10, no.2, pp.301-310, 2009.

[14] A. Rezai and P. Keshavarzi, " Speed Improvement in elliptic curve cryptosystem scalar multiplication algorithm," in proc. 7th international ISC conference on information security and cryptology,2010, pp.181-188.

[15] B. Qin, M. Li, F. Kong and D. Li, "New left-to-right minimal weight signed-digit radix-r representation," Computers & Electrical Engineering, vol. 35, no.1,pp. 150- 158,2009.

[16] X.Yin, H. Zhu and R. Zhao,"Window algorithm of scalar multiplication based on interleaving," in Proc. international conference on communications, circuits and systems, 2009, pp. 318- 321.

[17] G. Orlando and C. Paar, "A scalable GF(p) elliptic curve processor architecture for programmable hardware," in Proc. CHES01,2001, pp. 348- 363.

[18] A. Gutub and M. Ibrahim, "High radix parallel architecture for GF(p) elliptic curve processor," in proc. the IEEE Conference acoustics speech signal process, 2003, pp. 625- 628.

[19] C.K.Koc and C.Y.Hung, "Adaptive m-ary segmentation and canonical recoding algorithms for multiplication of large binary numbers," computer mathematic application, vol.24, no.3, pp.3- 12, 1992.

[20] G. M. Dormale and J. J. Quisquater, "High-speed hardware implementations of elliptic curve cryptography: a survey," Journal of systems architecture, vol.53, pp.72- 84, 2007.

[21] A. Rezai and P. Keshavarzi, "Improvement of high-speed modular exponentiation algorithm by optimum using smart methods," in proc. the 18th Iranian Conference on Electrical Engineering, 2010, pp.2104-2109.

[22] A. Rezai and P. Keshavarzi, "High-performance Modular Exponentiation Algorithm by Using a New Modified Modular Multiplication Algorithm and Common-Multiplicand-Multiplication Method", in Proc. The IEEE. World congress on internet security, 2011, pp. 192- 197.

[23] P. L. Montgomery, "Modular multiplication without trial division," Mathematics of computation, vol. 44, no.170, pp. 519- 521, 1985.

[24] L. Batina, et al. "Side channel attaks and fault attaks on cryptographic algorithm," Revue HF Tijdschrift, vol.3, pp. 36- 45, 2004.